CLAIM SCENARIO

RANSOMWARE | Retail Trade

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

An employee of a music instrument retailer accidentally clicked on a malware link. The virus was downloaded onto the company server causing all data to be encrypted. The employee then received an email demanding $50,000 paid in Bitcoin within 48 hours to release their data files.

2,000 customer records including name, address, phone, and credit card information were encrypted. The retailer called their insurance company's cyber response team, who responded by assigning a "breach coach," which is covered as part of the retailer's stand-alone cyber policy.

The breach coach sent in a forensics team to assess the situation, including any computer or electronic hardware damage, and determine if paying the ransom was necessary. Concurrently, the insurance company confirmed coverage and assisted with opening a claim to minimize the effect of business interruption.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Incident response manager ("breach coach") fees	$ 5,500
Forensic investigation costs to locate malware, analyze damage, ensure containment and calculate loss	$ 6,860
Legal fees	$ 4,000
NOTIFICATION COSTS	$ 1,230
BUSINESS INTERRUPTION	$ 31,325
DATA RECOVERY Costs associated with replacing lost or corrupted data	$ 10,100
EXTORTION/RANSOMWARE Ransom payment	$ 50,000
BRICKING Damage to computer and hardware systems	$ 12,050
TOTAL	$ 121,065

RESOLUTION

While the business maintained regular back-ups online, the hackers also encrypted these files leaving the retailer no way to restore the data. The insurance company and breach coach agreed the fastest, best way to get the business back up and running was to pay the ransom.

The insurance company immediately paid the ransom via their pre-established Bitcoin account, releasing the records back to the retailer.

The swift assessment and payment, minimized the business interruption allowing the retailer to resume operations.

CLAIM SCENARIO

OUTDATED SOFTWARE | Educational Services

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

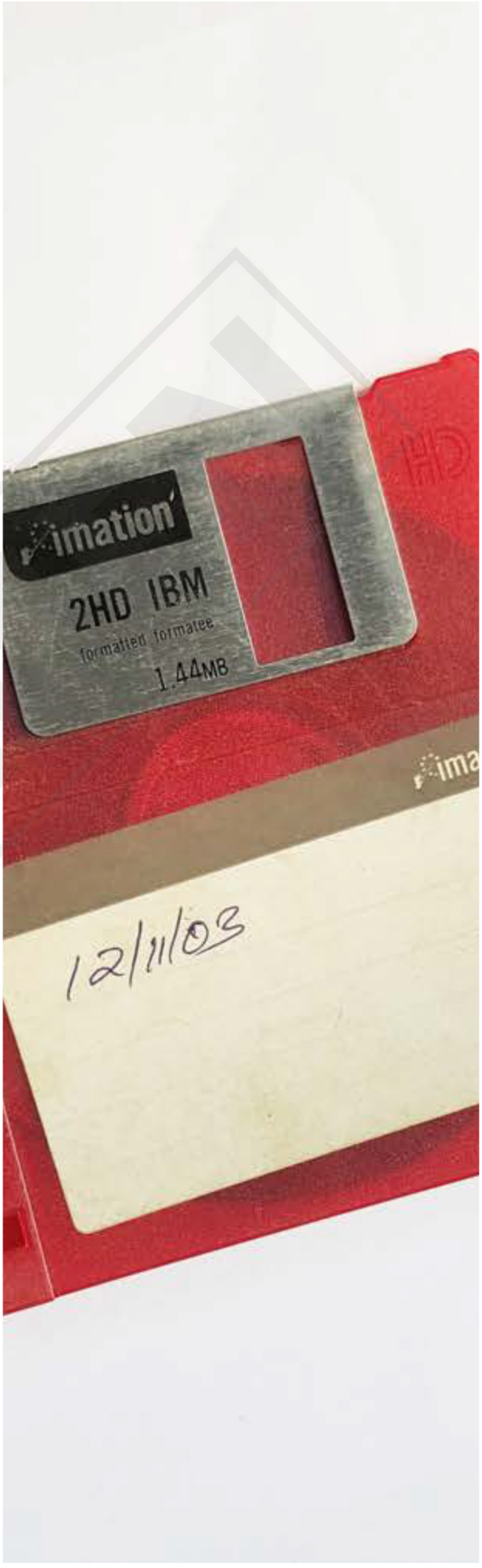
Hackers penetrated a graphic design school's network from a vulnerability in an outdated software application. 4,000 student names, addresses, emails, bank details and school records were compromised.

Local authorities received multiple complaints of suspicious activity, leading the school's IT department to discover an unauthorized user had accessed the system.

Once discovered, the school called their insurance carrier who immediately brought in forensic experts to initiate the school's IT recovery plan and notification program.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	$ 11,850
Identity theft and credit monitoring services	$ 11,500
Incident response fees	$ 7,850
Public relations fees to minimize reputational impact	$ 10,050
Call center set up and operation to field inquiries	$ 10,200
NOTIFICATION COSTS	$ 1,865
DATA RECOVERY Costs associated with replacing lost or corrupted data	$ 14,850
REGULATORY	
Legal expenses arising from regulatory investigation due to mismanagement of private information	$ 22,175
Legal expenses and settlement costs for claims	$ 16,100
Business interruption	$ 39,318
TOTAL	**$ 145,758**



RESOLUTION

The school's cyber policy was triggered, giving them immediate access to response services. The insurance company dispatched a forensic team who quickly isolated the unauthorized user.

A claim was started immediately to help with impending legal, consulting and media costs. The insurance company, IT team and forensic consultants ensured the school had up-to-date cyber defenses including firewalls, intrusion detection software, and encrypted databases. Concurrently, officials worked with local media to notify affected students and offer credit monitoring services, while the legal team handled the backlash from those affected.

Finally, the forensic consultants helped develop a new plan that included regular updates, testing, and education of all staff to minimize future breaches.

CLAIM SCENARIO

SOCIAL ENGINEERING | Finance and Insurance

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A mortgage broker's emails were accessed by an attacker who, posing as the General Manager, asked an employee to contact the broker's bank with instructions for funds to be transferred into the hacker's bank account.

When the mortgage broker discovered that unauthorized payments were made totaling $425,000, they immediately contacted their bank to freeze the funds and notified their cyber insurance carrier. Together, they were able to recover $354,000 of the unauthorized transactions.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to locate the breach, analyze damage, and ensure containment	**$ 13,500**
Legal fees	**$ 9,500**
FUNDS TRANSFER FRAUD Transferred funds not recovered	**$ 71,000**
TOTAL	**$ 94,000**

RESOLUTION

The mortgage broker has a stand-alone cyber policy that covers social engineering as well as provides crucial response services. Once the broker notified their insurance company, an IT forensic consultant was appointed to assist the broker in repairing the damage to their system as well as to prevent future attacks.

As the mortgage broker has expanded cyber crime coverage under their policy, they were reimbursed for the direct financial loss, less the deductible, of the unrecovered fraudulent transfers as well as their forensic and legal costs.

CLAIM SCENARIO

LOST HARDWARE | Health Care and Social Assistance

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

An employee of a medical group lost their laptop. An Excel file on the computer contained medical records of 1,500 patients including the names, addresses, dates-of-birth, medical record numbers, medications, and diagnoses.

Once the loss was realized, the medical group immediately notified their insurance company who provided a "breach coach" to assess the damage and help the insured comply with regulatory and notification requirements.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic costs to assess and contain damage	**$ 8,000**
Legal fees	**$ 15,500**
Public relations fees to minimize reputational impact	**$ 10,000**
NOTIFICATION COSTS	**$ 1,250**
DATA RECOVERY Costs associated with replacing lost or corrupted data	**$ 9,550**
REGULATORY Settlement fine	**$ 25,000**
Patient liability settlements	**$ 52,200**
TOTAL	**$ 121,500**

RESOLUTION

The breach coach assigned a forensics team, provided by the insurance company, to determine the potential exposure of the protected health information (PHI). It was determined that the patient PHI was, in fact, compromised. The patients were immediately notified and offered credit monitoring services.

Concurrently, the breach coach engaged a public relations agency to minimize the reputational damage as well as alerted counsel to help settle legal action from patients.

They were proactive in contacting the Department of Health and Human Service Office for Civil Rights and agreed upon a settlement amount as well as a corrective action plan that included employee cyber and data protection training.

CLAIM SCENARIO

FORMER OR ROGUE EMPLOYEE | Arts, Entertainment, and Recreation

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A museum was hacked by a former employee, whose user credentials were not deleted when they were terminated. The employee sold 1,115 donor records on the dark web including name, address, email, and credit card number including expiry dates.

The museum notified their insurance company immediately. The carrier provided forensic expertise, legal services, and media relations help to investigate and control the damage.

In addition, the insurance company enlisted a "breach coach" to guide the museum in managing their actual and reputational damage.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to analyze damage and ensure containment	**$ 7,600**
Identity theft and credit monitoring services	**$ 5,620**
Legal fees	**$ 9,935**
Public relations fees to minimize reputational impact	**$ 8,380**
Call center set up and operation to field inquiries	**$ 5,700**
NOTIFICATION COSTS	**$ 1,025**
DATA RECOVERY Costs associated with replacing lost or corrupted data	**$ 8,450**
TOTAL	**$ 46,710**

RESOLUTION

The forensic team quickly identified the breach and worked with the museum's IT department to initiate repairs. The breach coach guided the museum to hire a call center to quickly inform affected donors, field questions, and offer identity protection and credit monitoring services to ensure trust going forward. The insurance company recommended seeking legal counsel to pursue civil action against the former employee.

Concurrently, the museum, in tandem with the media relations team, responded quickly and transparently to the media.
Finally, the insurance company and forensic team recommended an updated cyber response plan that included more rigorous IT policies and procedures as well as several technological updates to improve cyber hygiene. Due to the fast response, the costs and reputational damage to the museum were minimized.